

COHN LIFLAND PEARLMAN
HERRMANN & KNOPF LLP
PETER S. PEARLMAN
Park 80 Plaza West-One
Saddle Brook, NJ 07663
Telephone: 201/845-9600
201/845-9423 (fax)

Liaison Counsel

COUGHLIN STOIA GELLER
RUDMAN & ROBBINS LLP
PAUL J. GELLER
DAVID J. GEORGE
JAMES L. DAVIDSON
BAILIE L. HEIKKINEN
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)

FARUQI & FARUQI, LLP
NADEEM FARUQI
EMILY C. KOMLOSSY
JAMIE R. MOGIL
369 Lexington Avenue, 10th Floor
New York, NY 10017-6531
Telephone: 212/983-9330
212/983-9331 (fax)

Co-Lead Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

DISTRICT OF NEW JERSEY

In re HEARTLAND PAYMENT
SYSTEMS, INC. SECURITIES
LITIGATION

This Document Relates To:

ALL ACTIONS.

) No. 3:09-cv-01043-AET-TJB
)
) CLASS ACTION
)
) PLAINTIFFS' MEMORANDUM OF
) LAW IN OPPOSITION TO
) DEFENDANTS' MOTION TO
) DISMISS

TABLE OF CONTENTS

	Page
I. PRELIMINARY STATEMENT	1
II. ARGUMENT	4
A. Legal Standards	4
B. The Complaint Sufficiently Identifies Actionable Misstatements	6
1. Defendants’ Failure to Disclose, and Outright Denial of the Occurrence of, the Security Breach was False and Misleading	8
2. Defendants’ Class Period Statements Concerning the General State of Security at Heartland were False and Misleading	13
3. Heartland’s “Warnings” to Investors were Illusory Because They Were Not Meaningful and They Warned of “Potential” Issues at a Time Defendants had Actual Knowledge of a Security Breach.....	15
4. Defendants’ Statements are Not Mere Corporate Puffery.....	18
C. The Complaint Adequately Alleges Scienter	21
1. The Pleading Standard for Scienter	21
2. Plaintiffs’ Inferences of Scienter are Cogent and Compelling.....	23
D. The Complaint Sufficiently Alleges Loss Causation	36
E. The Complaint Sufficiently Alleges Control Person Liability.....	39
III. CONCLUSION	40

TABLE OF AUTHORITIES

CASES

<i>ACA Fin. Guar. Corp. v. Advest, Inc.</i> , 512 F.3d 46 (1st Cir. 2008)	22
<i>Adams v. Amplidyne, Inc.</i> , No. CIV.A.99-4468, 2000 WL 34603180 (D.N.J. Oct. 24, 2000).....	28
<i>Asher v. Baxter Int’l, Inc.</i> , 377 F.3d 727 (7th Cir. 2004)	15
<i>Basic Inc. v. Levinson</i> , 485 U.S. 224 (1988)	9
<i>Blatt v. Corn Prods. Int’l, Inc.</i> , No. 05 C 3033, 2006 WL 1697013 (N.D. Ill. June 14, 2006).....	15
<i>Cal. Public Employees’ Ret. Sys. v. Chubb Corp.</i> , 394 F.3d 126 (3d Cir. 2004)	7
<i>Cal. Public Employees’ Ret. Sys. v. Chubb Corp.</i> , No. 00-4285, 2002 WL 33934282 (D.N.J. June 26, 2002)	16
<i>Cent. Laborers’ Pension Fund v. Integrated Elec. Servs. Inc.</i> , 497 F.3d 546 (5th Cir. 2007)	5
<i>Cosmas v. Hassett</i> , 886 F.2d 8 (2d Cir. 1989)	27
<i>Dura Pharms., Inc. v. Broudo</i> , 544 U.S. 336 (2005)	36, 37, 38
<i>EP Medsystems, Inc. v. EchoCath, Inc.</i> , 235 F.3d 865 (3d Cir. 2000)	37
<i>Ernst & Ernst v. Hochfelder</i> , 425 U.S. 185 (1976)	23
<i>Flynn v. Bass Bros. Enters.</i> , 744 F.2d 978 (3d Cir. 1984)	35

<i>Grossman v. Waste Mgmt., Inc.</i> , 589 F. Supp. 395 (N.D. Ill. 1984).....	34
<i>Heller v. Goldin Restructuring Fund, L.P.</i> , 590 F. Supp. 2d 603 (S.D.N.Y. 2008)	22
<i>In re Able Labs. Sec. Litig.</i> , No. CIV.A. 05-2681, 2008 WL 1967509 (D.N.J. March 24, 2008)	14
<i>In re Adams Golf, Inc. Sec. Litig.</i> , 381 F.3d 267 (3d Cir. 2004)	9, 10, 28, 29
<i>In re Advanta Corp. Sec. Litig.</i> , 180 F.3d 525 (3d Cir. 1999)	<i>passim</i>
<i>In re Aetna Inc. Sec. Litig.</i> , 34 F. Supp. 2d 935 (E.D. Pa. 1999).....	27
<i>In re Allaire Corp. Sec. Litig.</i> , 224 F. Supp. 2d 319 (D. Mass. 2002).....	34
<i>In re Alpha Pharma Inc. Sec. Litig.</i> , 372 F.3d 137 (3d Cir. 2004)	23
<i>In re Blockbuster Inc. Sec. Litig.</i> , No. 3:03-cv-0398-M, 2004 U.S. Dist. LEXIS 7173 (N.D. Tex. Apr. 26, 2004)	16
<i>In re Bradley Pharms., Inc. Sec. Litig.</i> , 421 F. Supp. 2d 822 (D.N.J. 2006).....	37, 39
<i>In re Burlington Coat Factory Sec. Litig.</i> , 114 F.3d 1410 (3d Cir. 1997)	6, 19, 21
<i>In re Cabletron Sys., Inc.</i> , 311 F.3d 11 (1st Cir. 2002)	23
<i>In re Cambrex Corp. Sec. Litig.</i> , No. 03-CV-4896, 2005 WL 2840336 (D.N.J. Oct. 27, 2005).....	19
<i>In re Countrywide Fin. Corp. Sec. Litig.</i> , 588 F. Supp. 2d 1132 (C.D. Cal. 2008).....	32, 33

<i>In re Daou Sys., Inc.,</i> 411 F.3d 1006 (9th Cir. 2005)	37
<i>In re Enron Corp. Sec., Derivative & ERISA Litig.,</i> 439 F. Supp. 2d 692 (S.D. Tex. 2006).....	37
<i>In re Indep. Energy Holdings PLC Sec. Litig.,</i> 154 F. Supp. 2d 741 (S.D.N.Y. 2001)	7
<i>In re Lernout & Hauspie Sec. Litig.,</i> 208 F. Supp. 2d 74 (D. Mass. 2002).....	26
<i>In re Lucent Techs, Inc. Sec. Litig.,</i> 217 F. Supp. 2d 529 (D.N.J. 2002).....	19
<i>In re Motorola Sec. Litig.,</i> 505 F. Supp. 2d 501 (D. Ill. 2007)	37
<i>In re NAHC, Inc. Sec. Litig.,</i> 306 F.3d 1314 (3d Cir. 2002)	9
<i>In re Nash Finch Co. Sec. Litig.,</i> 502 F. Supp. 2d 861 (D. Minn. 2007)	17
<i>In re OCA, Inc. Sec. & Deriv. Litig.,</i> No. 05-2165, 2006 U.S. Dist. LEXIS 90854 (E.D. La. Dec. 14, 2006).....	27
<i>In re Par Pharm. Sec. Litig.,</i> C.A. No. 06-cv-3226 (PGS), 2009 U.S. Dist. LEXIS 90602 (D.N.J. Sept. 30, 2009)	38, 39
<i>In re Party City Sec. Litig.,</i> 147 F. Supp. 2d 282 (D.N.J. 2001).....	23
<i>In re PeopleSoft, Inc., Sec. Litig.,</i> No. C99-00472, 2000 U.S. Dist. LEXIS 10953 (N.D. Cal. May 26, 2000)	27
<i>In re Schering-Plough Corp./Enhance Sec. Litig.,</i> No. CIV.A.08-CV-397, 2009 WL 2855457 (D.N.J. Sept. 2, 2009).....	5, 6
<i>In re Scottish Re Group Sec. Litig.,</i> 524 F. Supp. 2d 370 (S.D.N.Y. 2007)	32

<i>In re Tommy Hilfiger Sec. Litig.</i> , No. 04-Civ-7678, 2007 U.S. Dist. LEXIS 55088 (S.D.N.Y. July 20, 2007)	39
<i>In re Vivendi Universal, S.A. Sec. Litig.</i> , 381 F. Supp. 2d 158 (S.D.N.Y. 2003)	19
<i>Institutional Investors Group v. Avaya, Inc.</i> , 564 F.3d 242 (3d Cir. 2009)	<i>passim</i>
<i>Jaroslavicz v. Engelhard Corp.</i> , 704 F. Supp. 1296 (D.N.J. 1989)	34
<i>Lapin v. Goldman Sachs Group, Inc.</i> , 506 F. Supp. 2d 221 (S.D.N.Y. 2006)	21
<i>Lautenberg Found. v. Madoff</i> , No. CIV.A. 09-816, 2009 WL 2928913 (D.N.J. Sept. 9, 2009)	34
<i>Makor Issues & Rights, Ltd. v. Tellabs Inc.</i> , 513 F.3d 702 (7th Cir. 2008)	28, 33
<i>Malin v. XL Capital Ltd.</i> , 499 F. Supp. 2d 117 (D. Conn. 2007) <i>aff'd</i> , 2009 U.S. App. LEXIS 4984 (2d Cir. Mar. 5, 2009)	19
<i>Marangos v. Swett</i> , No. 08-4146, 2009 WL 1803264 (3d Cir. June 25, 2009)	6
<i>Nathenson v. Zonagen, Inc.</i> , 267 F.3d 400 (5th Cir. 2001)	27
<i>Novak v. Kasaks</i> , 216 F.3d 300 (2d Cir. 2000)	7, 20, 21
<i>Palladin Partners v. Gaon</i> , No. 05CV3305, 2006 WL 2460650 (D.N.J. Aug. 22, 2006)	23, 26
<i>Reina v. Tropical Sportswear Int'l</i> , No. 8:03-cv-1958, 2005 U.S. Dist. LEXIS 6129 (M.D. Fla. Apr. 4, 2005)	16
<i>Rombach v. Chang</i> , 355 F.3d 164 (2d Cir. 2004)	17

<i>Sheehan v. Little Switzerland, Inc.</i> , 136 F. Supp. 2d 301 (D. Del. 2001)	39
<i>South Ferry LP v. Killinger</i> , 542 F.3d 776 (9th Cir. 2008)	23
<i>Southland Sec. Corp. v. Inspire Ins. Solutions Inc.</i> , 365 F.3d 353 (5th Cir. 2004)	19
<i>Staffin v. Greenberg</i> , 672 F.2d 1196 (3d Cir. 1982)	35
<i>Steiner v. MedQuist, Inc.</i> , No. 04-5487, 2006 U.S. Dist. LEXIS 71952 (D.N.J. Sept. 29, 2006)	36
<i>Tellabs, Inc. v. Makor Issues & Rights, Ltd.</i> , 551 U.S. 308 (2007)	<i>passim</i>
<i>Weiner v. Quaker Oats Co.</i> , 129 F.3d 310 (3d Cir. 1997)	9
<i>Wiley v. Hughes Capital Corp.</i> , 746 F. Supp. 1264 (D.N.J. 1990).....	39
<i>Wilson v. Bernstock</i> , 195 F. Supp. 2d 619 (D.N.J. 2002).....	30, 31
<i>Winer Family Trust v. Queen</i> , 503 F.3d 319 (3d Cir. 2007)	5

STATUTES, RULES AND REGULATIONS

Rule 10b-5.....	4, 5, 39
15 U.S.C. §78j(b)	5
15 U.S.C. §78u-5(c)(1)(B)	16
17 C.F.R. §240.10b-5.....	5
Fed. R. Civ. P. 8.....	36, 40
Fed. R. Civ. P. 9(b)	4, 6, 8, 40
Fed. R. Civ. P. 12(b)(6).....	5, 6, 9

Co-Lead Plaintiffs Teamsters Local Union No. 727 Pension Fund and Genesee County Employees' Retirement System (collectively, "Plaintiffs") submit this memorandum of law in opposition to the motion to dismiss ("Motion" or "Def. Mem.") filed by Defendants Heartland Payment Systems, Inc. ("Heartland" or the "Company"), Robert O. Carr ("Carr") and Robert H.B. Baldwin ("Baldwin") (collectively, "Defendants").

I. PRELIMINARY STATEMENT

Having concealed a computer system breach that compromised approximately 130 million credit and debit card numbers and corresponding card data and decimated Heartland's intermediate-term business prospects, Defendants now try to use factual sleight-of-hand and misapplied legal principles in an attempt to convince this Court that Plaintiffs have not met the pleading requirements of the Private Securities Litigation Reform Act ("PSLRA"). Indeed, Defendants either ignore, mischaracterize, or ask the Court not to accept as true the myriad facts included in the Amended Consolidated Class Action Complaint for Violations of the Federal Securities Laws ("Complaint" or "Compl. at __"), then attempt to "bolster" their spurious arguments by saying there are literally *no facts* in the Complaint.

First, Defendants paint themselves as victims of a "sophisticated" and "clandestine" criminal "cyber-attack" on the Company's payment processing

system through “deeply hidden ‘malware.’” *See* Def. Mem. at 3. Then, Defendants ask the Court to decide a critical factual issue and accept their unsupported assertion that the security breach in 2007 (which Defendants now admit occurred, but never disclosed during the Class Period) was somehow separate and apart from the “cyber-attack” that was announced in January 2009. *See* Def. Mem. at 4. Of course, in order to convince the Court to do so, Defendants must and do ignore that this assertion has been refuted by Plaintiffs’ investigation, an Indictment issued by the United States Department of Justice (the “Indictment”), and by Defendants’ own post-Class Period statements. *See, e.g.*, Compl. at ¶¶75, 120, 122. Finally, Defendants attempt to discount the testimony of former employees of Heartland as to the pervasive security vulnerabilities at the Company and the resulting inability to prevent and remedy any security breach.¹

Setting their rhetoric aside, Defendants fall woefully short of overcoming the actual facts alleged in the Complaint, each of which is deemed to be true for purposes of the Court’s determination of the Motion:

¹ Ironically – given Defendants’ characterization of the well-supported allegations of the Complaint as conclusory – Defendants label Plaintiffs’ Confidential Witnesses as “disgruntled” former Heartland employees without any explanation whatsoever to support such name-calling. Apparently Defendants’ position is that any former employee who provides information about their fraud is “disgruntled.”

- as attested to by multiple former employees of Heartland (all of whom were in a position to know the information about which they spoke), the Company's Passport and Exchange systems (and more specifically, the Payroll Manager application where the security breach occurred) had undisclosed, pervasive security vulnerabilities throughout 2007 (*see, e.g.*, Compl. at ¶¶42, 44, 46-47, 49-52, 57);
- a security breach by way of an SQL Injection Attack in Heartland's Passport system occurred on **December 26, 2007**, as confirmed by a former Senior Developer at Heartland, and the Indictment (*see, e.g.*, Compl. at ¶¶4-6, 72-80, 122);
- Defendants were aware of this security breach by **December 30, 2007** by virtue of both direct knowledge of the breach, and because security was critical to the Company's core-operations as a credit-card payment processor (*see, e.g.*, Compl. at ¶¶49, 56, 78, 81, 120);
- Defendants did not take the steps necessary to remedy the breach, did not have the correct security measures in place to do so, and therefore did not successfully rectify the problem (*see, e.g.*, Compl. at ¶¶79-80, 85-90);
- ***Defendants outright denied publicly in February 2008 that a security breach had occurred at the Company in late 2007*** (*see* Compl. at ¶¶92, 93);
- Defendants continued to withhold from the market (***for over a year***) that a security breach had occurred at the Company in December 2007, even after they became aware of an almost identical SQL Injection Attack that had been publicly disclosed by another company, and after they were advised by Visa that suspicious fraudulent transactions were occurring from accounts linked to Heartland's systems (*see, e.g.*, Compl. at ¶¶97-101, 105);
- on **January 20, 2009** (Inauguration Day), Defendants announced to the market that a security breach had occurred at the Company and – though Defendants claimed they were unaware of when the breach had occurred – they believed that the malware from the breach ceased being active in 2008 (*see* Compl. at ¶¶108, 109);
- on January 22, 2009, Bloomberg published an article noting that ***the Company stated that the security breach occurred sometime in 2008*** (*see* Compl. at ¶111);

- in early August 2009, just days before the Indictment was to be issued which would reveal to the market that the SQL Injection Attack at Heartland that compromised 130 million consumers' card data actually occurred in *December 2007*, Defendants – for the first time – disclosed publicly that *the security breach had actually occurred in December 2007* (see Compl. at ¶120); and
- on August 17, 2009, the United States Department of Justice issued an Indictment indicating that the SQL Injection Attack on Heartland's computer network which resulted in the theft of 130 million credit card and debit card numbers and corresponding card data began on December 26, 2007 (see Compl. at ¶¶4, 122).

Despite Defendants' invitation to the Court to either ignore these *facts* or interpret them in a manner designed to resolve factual issues in favor of Defendants, these *facts* more than adequately satisfy the heightened pleading standards established by the PSLRA and Federal Rule of Civil Procedure 9(b). The Complaint details the falsity of Defendants' statements with particularity, provides specific facts, that, when viewed cumulatively and holistically, demonstrate Defendants' scienter, and adequately notifies Defendants of the causal link between their misrepresentations and the claimed losses. Defendants' efforts to minimize and gloss over the particularized factual allegations in the Complaint are unpersuasive, should be disregarded, and this Court should deny the Motion.

II. ARGUMENT

A. Legal Standards

Under §10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder, it is unlawful for any person, directly or indirectly, to commit fraud in connection

with the purchase or sale of securities. 15 U.S.C. §78j(b); 17 C.F.R. §240.10b-5. To state a claim for securities fraud under Rule 10b-5, plaintiffs must allege defendants made a misstatement or an omission of material fact with scienter in connection with the purchase or the sale of a security upon which plaintiffs reasonably relied and that plaintiff's reliance was the proximate cause of their injury. *Institutional Investors Group v. Avaya, Inc.*, 564 F.3d 242, 251 (3d Cir. 2009); *Winer Family Trust v. Queen*, 503 F.3d 319, 326 (3d Cir. 2007).²

“[F]aced with a Rule 12(b)(6) motion to dismiss a §10(b) action, courts must, as with any motion to dismiss for failure to plead a claim on which relief can be granted, accept all factual allegations in the complaint as true.” *Institutional Investors Group*, 564 F.3d at 252 (quoting *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007)); *see also Cent. Laborers' Pension Fund v. Integrated Elec. Servs. Inc.*, 497 F.3d 546, 551 (5th Cir. 2007) (“[T]he strong-inference pleading standard does not license us to resolve disputed facts at this stage of the case.”) Thereafter, courts must determine whether the complaint contains sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face. *In re Schering-Plough Corp./Enhance Sec. Litig.*, No. CIV.A.08-CV-397, 2009 WL 2855457, at *1 (D.N.J. Sept. 2, 2009). Facial

² Internal quotations and citations are omitted and all emphasis is added unless otherwise noted.

plausibility exists when the plaintiff pleads factual content “that allows the court to draw a reasonable inference that the defendant is liable for the misconduct alleged.” *Id.*; *see also Marangos v. Swett*, No. 08-4146, 2009 WL 1803264, at *2 (3d Cir. June 25, 2009).

The Motion challenges the Complaint for failure to properly plead several of these required elements, including material misrepresentations, scienter and loss causation. As discussed below, the Complaint satisfies the applicable pleading standards, and the Motion should be denied.

B. The Complaint Sufficiently Identifies Actionable Misstatements

On a motion to dismiss a federal securities fraud action, in addition to the well-settled Rule 12(b)(6) standards, the Court must also consider the heightened pleading standards of the PSLRA and Rule 9(b). *Schering-Plough*, 2009 WL 2855457, at *2.³ According to the Third Circuit, this means that the complaint must specify each allegedly misleading statement, why the statement was misleading, and, if an allegation is made on information and belief, all facts supporting that belief with particularity. *Institutional Investors Group*, 564 F.3d at 252. This standard merely “requires plaintiffs to plead the who, what, when, where

³ The heightened pleading standard of the PSLRA is relaxed somewhat where the factual information is peculiarly within the defendant’s knowledge or control. *In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1418 (3d Cir. 1997).

and how: the first paragraph of any newspaper story.” *Id.* (quoting *In re Advanta Corp. Sec. Litig.*, 180 F.3d 525, 534 (3d Cir. 1999)).

Unfortunately, as a result of these heightened pleading requirements, “motions to dismiss in securities fraud cases have become all too common where the procedural posture of the case renders most of the defendants’ arguments futile. Many motions to dismiss ask the court to engage in judgment calls which are better made by the trier of fact.” *In re Indep. Energy Holdings PLC Sec. Litig.*, 154 F. Supp. 2d 741, 747 (S.D.N.Y. 2001).⁴ The PSLRA does not require plaintiffs to plead with particularity every single fact upon which their claims concerning false or misleading statements are based. *Cal. Public Employees’ Ret. Sys. v. Chubb Corp.*, 394 F.3d 126, 146 (3d Cir. 2004) (quoting *Novak v. Kasaks*, 216 F.3d 300, 314 (2d Cir. 2000)). Rather, plaintiffs need only plead with particularity sufficient facts to support those beliefs. *Id.*

Here, Plaintiffs allege that Defendants – over the course of the Class Period – made numerous material misrepresentations and omissions concerning the pervasive security vulnerabilities at the Company, the security breach that occurred

⁴ As discussed more fully below, this is exactly what Defendants have done here. Defendants ask the Court to either disregard the facts alleged in the Complaint or interpret them according to Defendants’ desires – deciding factual issues in their favor and disregarding the mandate that the Court deem all factual allegations to be true for purposes of deciding a motion to dismiss.

at the Company in December 2007, and the Company's inability to remedy the breach. These allegations, supported by a wealth of source material and corroborated in various ways, easily satisfy the heightened pleadings standards of the PSLRA and Rule 9(b). Because the Complaint pleads the falsity of the misstatements with the particularity required by the PSLRA, Defendants' challenges are not well taken and should be disregarded.

1. Defendants' Failure to Disclose, and Outright Denial of the Occurrence of, the Security Breach was False and Misleading

Defendants have placed themselves between a rock and a hard place. Defendants refuse to admit that the December 2007 SQL Injection Attack (which they concealed for more than a year) and the security breach that Defendants finally disclosed in January 2009 are one in the same because such an admission would further support Plaintiffs' allegations that Defendants withheld material information concerning the security breach from the market. At the same time, the Indictment, Plaintiffs' investigation, and Carr's own statement to the news media (*i.e.*, the *facts*, as opposed to Defendants' convenient attempts to avoid liability through argument) undeniably establish that the security breach disclosed by Defendants in January 2009 (which compromised over 130 million consumers' credit and debit card information and other card data) and the SQL Injection Attack

which occurred at the Company in December 2007 are one and the same. *See, e.g.*, Compl. at ¶¶4-6, 72-80, 122.

Thus, in an attempt to escape from the factually damning quagmire they have created, Defendants have chosen to play fast and loose with the facts – manufacturing the subterfuge argument that the December 2007 SQL Injection Attack and the security breach disclosed by the Company in January 2009 are two different events. *See* Def. Mem. at 9.⁵ The acceptance of such argument by the Court would require the Court to abandon the mandate that all allegations in the Complaint be deemed true in the context of a motion to dismiss and to decide this

⁵ Even if the Court were to accept Defendants' unsupported factual allegation that the two breaches were completely unrelated – despite the fact that Plaintiffs' Confidential Witnesses, the Indictment and Carr's admissions say otherwise – Plaintiffs believe that Defendants still violated §10(b) by withholding from the market the fact that a security breach had occurred on the Company's databases. Heartland is in the business of processing credit card payments, and holds itself out to be in the business of protecting consumers' financial information – data security is at the very core of the Company's business. There would certainly be a substantial likelihood that a reasonable investor would have viewed a security breach on the Company's corporate system – even were it to not have led to any theft or damage – as having significantly altered the “total mix of information available to the investor.” *In re NAHC, Inc. Sec. Litig.*, 306 F.3d 1314, 1330 (3d Cir. 2002) (quoting *Basic Inc. v. Levinson*, 485 U.S. 224, 231-32 (1988)). Materiality is a uniquely factual inquiry that is not appropriate for resolution at the motion to dismiss stage. *See In re Adams Golf, Inc. Sec. Litig.*, 381 F.3d 267, 274 (3d Cir. 2004) (when a motion to dismiss is brought materiality is ordinarily an issue left to the factfinder and is therefore not typically a matter for Rule 12(b)(6) dismissal; *Weiner v. Quaker Oats Co.*, 129 F.3d 310, 317 (3d Cir. 1997) (“[T]he emphasis on a fact-specific determination of materiality militates against a dismissal on the pleadings.”)).

critical factual issue in Defendants' favor, neither of which are appropriate on a motion to dismiss.

Further ignoring the well-pled allegations of the Complaint, and inviting the Court to do the same, Defendants assert that the “*only* relevant information” that Defendants had prior to January 12, 2009 concerning a security breach was: (1) “that hackers had launched an SQL Injection Attack on the Company’s corporate system, which was separate from the card-processing network,” and that (2) “the Company had contained and remedied the attack.” *See* Def. Mem. at 9.⁶ Defendants then assert that “Plaintiffs never allege any fact of which they have knowledge to support a repeated allegation in the Complaint – that the SQL injection into the corporate system in December 2007 was the proximate cause of

⁶ Aside from being demonstratively false, Defendants’ assertion that “[b]ecause the attack was thought to be contained without damage, this information did not significantly change the total mix of information available to investors concerning Heartland” should not be well-received on a motion to dismiss. Only if the alleged misrepresentations or omissions are so obviously unimportant to an investor that reasonable minds cannot differ on the question of materiality is it appropriate for the Court to rule that the allegations are inactionable as a matter of law. *Adams Golf Sec. Litig.*, 381 F.3d at 274-75. As the success of Heartland’s business depended almost entirely on its ability to maintain the absolute security of its customer’s confidential credit card information, Defendants’ raw conclusion, together with its unilateral proclamation that its failure to disclose the December 2007 SQL Injection was not material, defies logic.

the intrusion into the payment processing system announced by Heartland 13 months later on January 20, 2009.” *See* Def. Mem. at 5 n.7.

Defendants’ statements might be compelling if they did not contradict the actual facts. Conveniently, Defendants’ assertions omit several crucial details. For one, as alleged in the Complaint, Carr himself has already admitted that the “two” security breaches are actually the same breach:

Heartland’s CEO Robert Carr told Wired.com recently that the initial breach into the company’s network in December 2007 was confined to the company’s corporate network, which Carr said was separate from its card-processing network. But by May 2008, the hackers had jumped to the processing network. Carr wouldn’t say how they accomplished this (emphasis added).

See Compl. at ¶120. Further, the Indictment corroborates Carr’s statement that there was only one security breach at Heartland, and that it began in December 2007:

[b]eginning on or about ***December 26, 2007***, Heartland was the victim of an ***SQL Injection Attack*** on its corporate computer network ***that resulted in malware being placed on its payment processing system and the theft of more than approximately 130 million credit and debit card numbers and corresponding Card Data*** (emphasis added).

See Compl. at ¶121.⁷

⁷ As set forth in detail in the Complaint, Defendants had actual knowledge of the security breach as early as December 2007. Their subsequent denials that a breach had occurred, their failure to admit that the breach had occurred for over a year (until January 2009 – and even then stating that they were unaware of when the breach had occurred), their stunning admission just days before the issuance of

Defendants' premise is therefore not simply flawed, but demonstratively false. Clearly, there was one SQL Injection Attack, and, according to Defendants' own admission, it occurred in December 2007. The malware placed on Heartland's systems through the security breach remained on the Company's databases until at least January 2009, and led to the theft of more than approximately 130 million credit and debit card numbers and corresponding card data. In the words of the former Senior Developer cited in the Complaint, the Company "*didn't successfully annihilate the 2007 breach problem.*" See Compl. at ¶80.⁸

the Indictment that the breach actually occurred in December 2007, and the confirmation and corroboration by the Indictment that the breach disclosed by the Company in January 2009 actually occurred in December 2007, taken in their totality, justify the Court in drawing the inference that Defendants knew that the security breach that occurred in December 2007 at Heartland and the one that Defendants finally and begrudgingly announced in January 2009 were one in the same.

⁸ Defendants misread the Complaint in asserting that "Plaintiffs do not dispute their own CW's belief that the intrusion into the payment processing system seems to have occurred no earlier than May 2008." See Def. Mem. at 18 n.15. The Confidential Witness referenced by Defendants did not state that it was her/his belief that the security breach occurred no earlier than May 2008. Rather, the Confidential Witness stated that "she/he believed it possible that the hackers who breached Heartland in late 2007 were able to insert the code that led to the credit card and debit cards thefts *the Company claims* began in May 2008." See Compl. at ¶77.

2. Defendants' Class Period Statements Concerning the General State of Security at Heartland were False and Misleading

Defendants next argue that the vulnerabilities detailed in the Complaint are immaterial because Plaintiffs have not connected the vulnerabilities to the security breach. *See* Def. Mem. at 10. Once again, Defendants ignore the facts as alleged in the Complaint.

The Complaint sets forth substantial evidence of significant vulnerabilities in the Company's Passport corporate network, where merchant data is stored and payment processing occurs ("Passport"). (*See* Compl. at ¶44: "[t]here was no security, no compliance, reporting or banking support. There were lots of little problems [with Passport]"; ¶46: "[t]here were very serious vulnerabilities in Passport.") According to Defendants' own admission, the security breach at the Company in December 2007 began in Passport (which the Company sometimes refers to as the "corporate network"). *See* Compl. at ¶120.

According to Defendants' Motion, the Passport corporate system contains an application called Payroll Manager. *See* Def. Mem. at 6. The Complaint specifically details the vulnerabilities in the Company's Payroll Manager application. *See* Compl. at ¶71. The former Heartland Senior Developer cited in the Complaint stated that the security breach occurred because the hackers were

able to exploit a vulnerability in Heartland's Payroll Manager application. *See* Compl. at ¶74.

So assuming the well-pled allegations of the Complaint to be true (as this Court must do on a motion to dismiss), and based, in part, upon Defendants' own admissions, the security breach began in Passport's Payroll Manager application. Furthermore, both the Payroll Manager application, and the Passport system itself (which contained the Payroll Manager application) had pervasive and significant security vulnerabilities, none of which were disclosed at any time by Defendants.

The most reasonable and plausible inference that can be drawn from these facts is that the pervasive security vulnerabilities detailed in the Complaint concerning the Payroll Manager application and the Passport corporate system were the proximate cause of the security breach into the Passport corporate system. *In re Able Labs. Sec. Litig.*, No. CIV.A. 05-2681, 2008 WL 1967509 (D.N.J. March 24, 2008) (on a motion to dismiss, all reasonable inferences must be drawn in plaintiff's favor). Defendants have not offered any other reasonable explanation to the contrary.⁹ Thus, Defendants' assertions that their statements concerning the

⁹ Notwithstanding Defendants' bald assertions that the false and misleading statements made by Defendants on March 10, 2008 related solely to security on the payment processing system where card data is handled (which the Company sometimes refers to as the "Exchange" system), a cursory glance at the portion of the March 10, 2008 10-K alleged to be false and misleading reveals that the statements made are about the overall security at Heartland, inclusive of both

Company's security were not false and misleading are without merit and should be rejected.

3. Heartland's "Warnings" to Investors were Illusory Because They Were Not Meaningful and They Warned of "Potential" Issues at a Time Defendants had Actual Knowledge of a Security Breach

Defendants next argue that any alleged misstatements about the SQL Injection Attack are inactionable because they were "forward-looking statements" accompanied by "meaningful cautionary language," and thus fall under the statutory "safe harbor" provided by the PSLRA. *See* Def. Mem. at 12. But the PSLRA "safe harbor" does not provide Defendants with the broad immunity they seek.¹⁰

Passport and Exchange. (*See* Compl. at ¶95: "[i]n the course of our operations, we compile and maintain a large database of information *relating to our merchants* and their transactions"; ¶95: "[o]ur internal network configuration provides multiple layers of security to isolate *our databases* from unauthorized access..."; ¶95: [i]f the Company's network is breached or sensitive *merchant* or cardholder data is misappropriated, the Company could be exposed to assessments, fines or litigation costs." Thus, Defendants' contention that the Complaint does not adequately allege that the statements in paragraph 95 are in any way inaccurate is without merit.

¹⁰ As an initial matter, Defendants' argument for safe harbor protection is premature. *See Asher v. Baxter Int'l, Inc.*, 377 F.3d 727, 734 (7th Cir. 2004) (reversing trial court's granting of motion to dismiss). As the Court found in *Asher*, because the language of safe harbor is so malleable, it is unsuitable to apply on a motion to dismiss. *Id.* ("There is no reason to think – at least, no reason that a court can accept at the pleading stage, before plaintiffs have access to discovery – that the items mentioned in [Defendants'] cautionary language were those" that were realized when the truth emerged. *Id.*; *see also Blatt v. Corn Prods. Int'l, Inc.*,

The PSLRA safe harbor is inapplicable because the Complaint demonstrates that when Defendants made the purported forward-looking statements, they were made “with actual knowledge.” 15 U.S.C. §78u-5(c)(1)(B); *see Advanta*, 180 F.3d at 536. In other words, the safe harbor provision does not afford corporations a free pass to lie to investors. *Cal. Public Employees’ Ret. Sys. v. Chubb Corp.*, No. 00-4285, 2002 WL 33934282, at *11 (D.N.J. June 26, 2002). Further, purposeful omissions of existing facts or circumstances do not qualify as forward-looking statements and are not protected by the safe harbor of the Reform Act. *Id.*

Consequently, despite the protections otherwise available under the PSLRA’s safe harbor, “[a] defendant remains liable even for a forward-looking statement, if the plaintiff shows that the defendant ‘knew at the time of the statement of false and misleading content and thus lacked a reasonable basis for making the statement.’” *Reina v. Tropical Sportswear Int’l*, No. 8:03-cv-1958, 2005 U.S. Dist. LEXIS 6129, at *23 (M.D. Fla. Apr. 4, 2005); *see also In re Blockbuster Inc. Sec. Litig.*, No. 3:03-cv-0398-M, 2004 U.S. Dist. LEXIS 7173, at *19-*20 (N.D. Tex. Apr. 26, 2004) (“If the representation or omission is fraudulent, independent of the existence of a forward-looking statement, the

No. 05 C 3033, 2006 WL 1697013, at *5 (N.D. Ill. June 14, 2006) (“[W]hether the cautions at issue here were adequate is a not [sic] question to be answered on a motion to dismiss. The sufficiency of Defendants’ cautionary tone (if, indeed, one was required) is a question of fact, or possibly a question of law, that can be answered only on a more developed record.”).

representation or omission is not shielded simply because a forward-looking statement exists.”).

Here, at the time that Defendants’ purportedly “meaningful” cautionary statements were made, Defendants knew (but failed to disclose) that the Company had incurred a significant and material security breach in December 2007, and had not, and was not capable of fully resolving the issues arising out of the breach. *See, e.g.*, Compl. at ¶¶73-80, 94. In other words, at the time that Defendants stated that “[o]ur computer systems could be penetrated by hackers” (*see, e.g.*, Compl. at ¶95), Defendants already knew that their computer systems had been penetrated by hackers, and the penetration had not been rectified. *See In re Nash Finch Co. Sec. Litig.*, 502 F. Supp. 2d 861, 873 (D. Minn. 2007) (“[I]f Defendants knew that the specific risks and uncertainties stated to be ‘potential’ in their cautionary language had already been realized, and that their forward-looking statements were false or misleading, then their forward-looking statements are not protected by the safe harbor.”). As such, Defendants’ purported “warnings” to investors were wholly inadequate. *See Rombach v. Chang*, 355 F.3d 164, 173 (2d Cir. 2004) (the safe harbor doctrine “provides no protection to someone who warns his hiking

companion to walk slowly because there might be a ditch ahead when he knows with near certainty that the Grand Canyon lies one foot away.”)¹¹

4. Defendants’ Statements are Not Mere Corporate Puffery

Defendants claim that three of the statements that Plaintiffs challenge are “inactionable corporate puffery.” *See* Def. Mem. at 13. This argument, quite frankly, ignores the well-pled allegations in the Complaint. Defendants knew that their optimistic statements had no basis in fact, and that these statements were actually contradicted by Defendants’ knowledge of the security breach and their inability to remedy the breach.

The Third Circuit has defined puffery as “vague and general statements of optimism ... understood by reasonable investors as such.” *Advanta*, 180 F.3d at 538. Such “statements of subjective analysis or extrapolation, such as opinions, motives and intentions” or other types of “soft information” are not actionable because investors do not rely on such information in making decisions. *Id.* at 539. “Opinion statements are actionable, however, if Plaintiffs can plead with

¹¹ Defendants incorporate into the Motion Exhibits A, B, and E-G to the Declaration of Stephen M. Orlofsky in Support of Defendants’ Motion to Dismiss Plaintiffs’ Amended Consolidated Class Action Complaint for the purpose of attempting to show this Court that they adequately warned investors about the risk of a security breach at the Company. *See, e.g.*, Def. Mem. at 11. As discussed more fully above, none of these purported “warnings” contain meaningful cautionary language given that Defendants had actual knowledge of the security breach and the pervasive security vulnerabilities at the Company at the time these statements were made.

particularity that defendants did not sincerely believe the opinion they purported to hold, or if they are worded as guarantees or are supported by specific statements of fact.” *Malin v. XL Capital Ltd.*, 499 F. Supp. 2d 117, 144-45 (D. Conn. 2007) *aff’d*, 2009 U.S. App. LEXIS 4984 (2d Cir. Mar. 5, 2009).¹²

The context in which optimistic statements are made is critical to the distinction between misrepresentation and puffery. *In re Lucent Techs, Inc. Sec. Litig.*, 217 F. Supp. 2d 529, 559 (D.N.J. 2002). In general, the more the statement diverges from known facts about the entity or the more precise and concrete the statement, the less likely courts have been to dismiss the statement as inactionable puffery. *See Southland Sec. Corp. v. Inspire Ins. Solutions Inc.*, 365 F.3d 353, 372 (5th Cir. 2004).¹³

Contrary to Defendants’ “puffery” argument, the Complaint pleads numerous objectively verifiable misrepresentations concerning, *inter alia*, the

¹² Whether the opinion or soft information is indeed actionable depends on all relevant circumstances of the particular case, and is generally not an appropriate basis on which to dismiss a complaint at this stage of the litigation. *In re Vivendi Universal, S.A. Sec. Litig.*, 381 F. Supp. 2d 158, 182 (S.D.N.Y. 2003).

¹³ The source of the statement also plays a role in determining if general statements of optimism are actionable. Statements of opinion by top corporate officials may be actionable if they are made without a reasonable basis. *In re Cambrex Corp. Sec. Litig.*, No. 03-CV-4896, 2005 WL 2840336, at *6 (D.N.J. Oct. 27, 2005). Courts distinguish such statements from ordinary, unattributed expressions of optimism because such statements can be materially significant to investors because investors know that these top officials have knowledge and expertise far exceeding that of the ordinary investor. *Burlington*, 114 F.3d at 1428.

security breach and the Company's inability to remedy the breach. *See, e.g.*, Compl. at ¶¶73-80, 94. *See, e.g., Novak*, 216 F.3d at 315 ("Here, the complaint alleges that the defendants did more than just offer rosy predictions; the defendants stated that the inventory situation was 'in good shape' or 'under control' while they allegedly knew that the contrary was true."). When comparing the statements that Defendants challenge as puffery, to what was known to Defendants at the time that the statements were made, Defendants' puffery arguments are without merit.

Defendants assert that their statements that they had a very secure system, that they placed a significant emphasis on security, and that security is a major driver are inactionable puffery. *See* Def. Mem. at 12-13.¹⁴ Defendants argue that these statements are the kind of vague statements that cannot support a securities claim. *Id.* at 13-14. Defendants are incorrect.

Rather than vague and general statements of optimism, the above-referenced statements are highly particularized, worded as guarantees, and misrepresent existing facts – namely that the Company did not place significant emphasis on security and the Company's systems were not at all secure at the time the

¹⁴ These statements, of course, directly contradict statements from Plaintiffs' Confidential Witnesses. *See, e.g.*, Compl. at ¶57 (data security was "***nothing [the Defendants] ever cared about. To claim now they always cared about it is very hypocritical from how they acted in the past. It is very, very contradictory to how they always acted.***"); ¶82 ("***security was not there***")

statements were made. *See, e.g.*, Compl. at ¶¶40-57, 69-84, 123-24.¹⁵ As such, these statements are actionable. *See Novak*, 216 F.3d at 315 (“While statements containing simple economic projections, expressions of optimism, and other puffery are insufficient, defendants may be liable for misrepresentations of existing facts.”).¹⁶

C. The Complaint Adequately Alleges Scienter

1. The Pleading Standard for Scienter

In a securities fraud action, with respect to each act or omission, the Complaint must state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind. *Institutional Investors Group*, 564 F.3d at 253. A “strong inference” of scienter is one that is “cogent and at least as compelling as any opposing inference of nonfraudulent intent.” *Tellabs*, 551

¹⁵ To the extent that Defendants argue that the Company did place significant emphasis on security and that its systems were secure at the time these statements were made, those assertions create factual disputes with the well-pled allegations of the Complaint, and thus are not properly disposed of on a motion to dismiss. *Burlington*, 114 F.3d at 1421.

¹⁶ At a minimum, given the context in which they were proactively affirmed and repeated, these statements “implied certainty” in the opinions held by Defendants, and are actionable. *Id.*; *Lapin v. Goldman Sachs Group, Inc.*, 506 F. Supp. 2d 221, 240 (S.D.N.Y. 2006) (“[T]he Second Amended Complaint does more than identify rosy predictions or vague statements about Goldman’s integrity; Goldman stated that such integrity ‘was at the heart’ of its business and attempted to distinguish itself from other institutions based on its ‘truly independent investment research’ while it allegedly knew the contrary was true.”).

U.S. at 314; *see also id.* at 2510 (“The inference that the defendant acted with scienter need not be irrefutable, *i.e.*, of the ‘smoking-gun’ genre, or even the most plausible of competing inferences.”)¹⁷ In each of these formulations, the Supreme Court effectively held that “ties” go to the plaintiff. *See, e.g., ACA Fin. Guar. Corp. v. Advest, Inc.*, 512 F.3d 46, 59 (1st Cir. 2008) (“[W]here there are equally strong inferences for and against scienter, Tellabs now awards the draw to the plaintiff.”); *Heller v. Goldin Restructuring Fund, L.P.*, 590 F. Supp. 2d 603, 620 n.14 (S.D.N.Y. 2008) (“Tellabs clearly stands for the proposition that, if an ‘inference of non fraudulent intent is equally permissible as any inference of fraudulent intent,’ the complaint is properly pleaded.”).

The pertinent question is “whether all of the facts alleged, taken collectively, give rise to a strong inference of scienter, not whether any individual allegation, scrutinized in isolation, meets that standard.” *Tellabs*, 551 U.S. at 323; *see also id.* at 310 (“[T]he court’s job is not to scrutinize each allegation in isolation but to assess all the allegations holistically.”). Accordingly, a court’s scienter analysis will ultimately rest not on the presence or absence of certain types of allegations but on a practical judgment about whether, accepting the whole factual picture

¹⁷ In the Motion, Defendants misstate this standard. *See* Def. Mem. at 4 (“Plaintiffs thus do not (as they must) plead facts that give rise to a compelling inference that any Defendants knew or recklessly disregarded...”)

painted by the Complaint, it is at least as likely as not that defendants acted with scienter. *Institutional Investors Group*, 564 F.3d at 253.¹⁸

2. Plaintiffs' Inferences of Scienter are Cogent and Compelling

a. Defendants Acted Consciously or, at a Minimum, Recklessly Disregarded the True State of Affairs at Heartland

Scienter is a “mental state embracing intent to deceive, manipulate, or defraud,” *Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 193 n.12 (1976), and requires a knowing or reckless state of mind, *Advanta*, 180 F.3d at 534-35. The complaint may present a “strong inference” of scienter “by alleging facts that constitute strong circumstantial evidence of ... recklessness.” *In re Alparma Inc. Sec. Litig.*, 372 F.3d 137, 148 (3d Cir. 2004). To survive dismissal, it is sufficient for plaintiffs to allege that defendants had knowledge of facts or access to information contradicting their public statements. *In re Party City Sec. Litig.*, 147 F. Supp. 2d 282, 315 (D.N.J. 2001); *Palladin Partners v. Gaon*, No. 05CV3305, 2006 WL 2460650, at *11 (D.N.J. Aug. 22, 2006).

¹⁸ See also *South Ferry LP v. Killinger*, 542 F.3d 776, 784 (9th Cir. 2008) (“Tellabs counsels us to consider the totality of circumstances, rather than to develop separately rules of thumb for each type of scienter allegation.”); *In re Cabletron Sys., Inc.*, 311 F.3d 11, 32 (1st Cir. 2002) (“Each securities fraud complaint must be analyzed on its own facts; there is no one-size-fits-all template.”).

(1) Defendants Knew that an SQL Injection Attack had Occurred in Passport, that Improper “linkages” Existed Between Passport and Exchange, and that Pervasive Security Vulnerabilities Continued to Exist at Heartland

Again ignoring the allegations in the Complaint, Defendants assert that “Plaintiffs plead no facts in support of the inference that Defendants believed that the SQL Injection Attack had not been remedied or that card data was at risk.” *See* Def. Mem. at 18. Defendants are incorrect.

The Complaint clearly alleges that an SQL Injection Attack occurred at Heartland in December 2007. *See* Compl. at ¶¶69-84. Defendants do not deny this fact, and it is corroborated by the Indictment. *See, e.g.,* Compl. at ¶4. The Complaint further alleges that the attack occurred in the Payroll Manager application in the Company’s Passport system. *See* Compl. at ¶74. A former Heartland Senior Developer – *who was in charge of the Payroll Manager application at the time of the security breach* – stated that Heartland did not correctly address the security breach, and did not remedy the problem. *See* Compl. at ¶¶70, 79-80.¹⁹ The Company’s failure to remedy the breach is corroborated by Defendants’ partial revelation of the truth at the end of the Class Period, and the subsequent admission that approximately 130 million consumers credit and debit

¹⁹ If the individual actually in charge of the Payroll Manager application knew that the breach was not remedied, then it is implausible to believe that Defendants thought that it was remedied.

card information and accompanying card data had been compromised. *See* Compl. at ¶¶108-09, 111, 120.

In the months following the security breach, Defendants, with full knowledge of the breach and its ramifications, failed to either disclose the breach or correct the pervasive security vulnerabilities at the Company. *See* Compl. at ¶¶56-57, 79-80, 85-89, 111. Indeed, while Defendants *claim* that the hackers had launched an SQL Injection Attack on the Company’s corporate system – which they state was separate from the Company’s card-processing network (thus attempting to imply that during the Class Period Defendants knew of a security breach but that it had nothing to do with the card-processing network) – Defendants admitted on the February 2008 conference call that there were “unnecessary linkages” between the corporate system and the card-processing system which they purportedly attempted to “fix.” *See* Compl. at ¶93.²⁰

Unfortunately for Plaintiffs, the Class and 130 million consumers, as has now been revealed, Defendants did not repair the “linkages” between the corporate network and the card processing network, and Defendants did not “[contain] and [remedy]” the security breach. Rather, as Defendants now admit, the hackers

²⁰ Defendants’ assertion that “the Complaint inappropriately leaps with the benefit of hindsight from the December 2007 attack to the later potential exposure of card data without pleading *any* facts showing that Defendants believed that a link existed *at the time*” wholly ignores this admission by Defendants.

“jumped” from the corporate network to the card-processing network, resulting in the largest data security breach in the history of the United States. *See* Compl. at ¶120.²¹

(2) The Core Business Doctrine – Defendants Are Presumed to Know About Facts Impacting the Cornerstone of Their Business

A strong inference of scienter can be inferred here because the alleged misrepresentations relate to data security at Heartland, which was at the very core of the Company’s business and drove earnings during the Class Period. *See, e.g., Palladin*, 2006 WL 2460650, at *12 (“[w]here fraud involves a company’s core business, knowledge or recklessness can be inferred from a defendant’s position in the company and related exposure and access to information revealing the fraud”);

²¹ Defendants do not dispute that particularized allegations of former employees “add to the inference of scienter” required under the PSLRA. *See, e.g., In re Lernout & Hauspie Sec. Litig.*, 208 F. Supp. 2d 74, 87 (D. Mass. 2002). Yet, much like their attack on falsity, Defendants raise fact-based arguments going to the credibility of Plaintiffs’ Confidential Witnesses, not whether they are properly identified. *See* Def. Mem. at 20 n.16. Furthermore, Defendants’ attack on Plaintiffs’ Confidential Witnesses, particularly Defendants’ argument that the former Senior Developer cited in the Complaint did not have “*any* knowledge of the payment processing system or card data,” contradicts the well-pled allegations of the Complaint. *Id.* In fact, the former Senior Developer cited in the Complaint ***was in charge of the Payroll Manager application on the Company’s corporate network, where the breach occurred, prior to and at the time that said breach occurred.*** *See* Compl. at ¶70. Moreover, Plaintiffs’ witnesses describe, based on personal knowledge, events at Heartland that were completely at odds with Defendants’ public statements. *See, e.g.,* Compl. at ¶¶40-57, 69-84. In turn, they demonstrate numerous “red flags” that Defendants, at a minimum, recklessly disregarded.

Cosmas v. Hassett, 886 F.2d 8, 12-13 (2d Cir. 1989) (allegations that sales to China were significant to company's business gave rise to strong inference that directors knew of Chinese import restrictions). That is, courts have repeatedly drawn the inference that "facts critical to a business's core operations or an important transaction generally are so apparent that their knowledge may be attributed to the company and its key officers." *In re PeopleSoft, Inc., Sec. Litig.*, No. C99-00472, 2000 U.S. Dist. LEXIS 10953, at *10 (N.D. Cal. May 26, 2000).²²

While it is true that knowledge of every piece of company information cannot be imputed to a defendant merely because of his or her position at that company, a court may factor in the position of the defendant as circumstantial evidence when the information is of great importance to the company. *See In re Aetna Inc. Sec. Litig.*, 34 F. Supp. 2d 935, 953 (E.D. Pa. 1999) (distinguishing *Advanta* on the grounds that "the alleged fraud did not relate to the corporation's core business," whereas "the alleged fraud in this case relates to the core business"). On remand from the Supreme Court, the Seventh Circuit in *Tellabs*

²² *See also Nathenson v. Zonagen, Inc.*, 267 F.3d 400, 425 (5th Cir. 2001) (scienter element satisfied as to patent statement because information regarding patent protection was "obviously important," critical to company's core performance, and about which the company had "ample opportunity to become familiar"); *In re OCA, Inc. Sec. & Deriv. Litig.*, No. 05-2165, 2006 U.S. Dist. LEXIS 90854, at *60-*64 (E.D. La. Dec. 14, 2006) (scienter properly alleged where defendants materially overstated value of company's largest asset).

recognized it is “exceedingly unlikely” that top executives did not know facts about the corporation’s “most important products,” particularly where they communicated with the market about those products. *See Makor Issues & Rights, Ltd. v. Tellabs Inc.*, 513 F.3d 702, 709, 711 (7th Cir. 2008) (“*Tellabs II*”).

The instant case is analogous to *Adams v. Amplidyne, Inc.*, No. CIV.A.99-4468, 2000 WL 34603180 (D.N.J. Oct. 24, 2000). In *Adams*, the defendants moved to dismiss a securities fraud complaint on the grounds, *inter alia*, that the Complaint failed to adequately allege scienter as it did not plead strong circumstantial evidence of conscious misbehavior or recklessness as required by Section 10(b). *Id.* at *7. The Court disagreed, finding that the plaintiffs’ core business allegations constituted circumstantial evidence of conscious behavior:

Plaintiffs allege the defendants had knowledge of the falsity of the statements by virtue of their positions within the company. The alleged misstatements and omissions concern the launch of a new wireless Internet access communications product by Amplidyne. Creating and marketing such products is central to Amplidyne’s core business. Thus, the facts and statements surrounding the product development can be attributed to high-level personnel such as officers and directors. Plaintiffs allege that Bains is, and was at all relevant times, the Chief Executive Officer, President, Principal Accounting Officer, Treasurer, and a director of Amplidyne. They further allege that Bains was involved in the day-to-day operation of Amplidyne, privy to confidential proprietary information concerning its business, and was involved in the writing, reviewing, and disseminating of the materially false information. This level of involvement supports the notion that Bains either knew or should have known of the misstatements involved. His close day-to-day involvement with the operation of Amplidyne and the launch of the new products strongly supports an inference of scienter.

Id.

Here, as in *Adams*, the Complaint alleges that each of the Individual Defendants, as senior executive officers and/or directors of Heartland, were privy to non-public information concerning the Company's business, finances, products, markets and present and future business prospects via access to internal corporate documents, conversations and connections with other corporate officers and employees, attendance at management and Board of Directors meetings and committees thereof and via reports and other information provided to them in connection with those meetings. *See* Compl. at ¶24. The Complaint further alleges that the security of Heartland's systems, and the protection of consumers' private, personal information, was absolutely critical to Heartland's core business. *See, e.g.,* Compl. at ¶¶49, 81.

Defendants cannot legitimately dispute the importance of data security to the Company's operations. The protection of consumers' private, personal information is at the core of any business that specializes in credit card payment processing. Indeed, throughout the Class Period, Defendants made repeated statements referencing the importance of data security to the Company. *See* Compl. at ¶¶91-93, 95, 100. These included Defendants' repeated (and false) proclamations that "[w]e place significant emphasis on maintaining a high level of

security in order to protect the information of our merchants and their customers.”

See Compl. at ¶96.

As Defendants held themselves out as placing a significant emphasis on data security, it defies belief that the Individual Defendants, as executives of Heartland, did not know that a “sophisticated” security breach had occurred on the Company’s systems. Indeed, as the Complaint alleges, Heartland’s Chief Technology Officer and Heartland’s Executive Director of I.T. knew of the security breach as early as January 2008, and probably before that time. *See* Compl. at ¶81. Further, the Company made attempts (albeit, feeble ones) to remedy the security breach, including blocking its database server from transmitting data to I.P. addresses in the Netherlands. *See* Compl. at ¶¶75-76.

Additionally, several Heartland employees, including the former Senior Software Developer and the former Senior Programmer referenced in the Complaint, advised Heartland’s Chief Technology Officer of security vulnerabilities in Passport. *See* Compl. at ¶49. Furthermore, the physical security at the Company’s offices was non-existent – a fact that could not have gone unnoticed by Defendants, who worked in those very offices. *See* Compl. at ¶¶53-55.

Defendants cite one case, *Wilson v. Bernstock*, 195 F. Supp. 2d 619 (D.N.J. 2002), in a footnote, in an attempt to contradict Plaintiff’s core-business

allegations. *See* Def. Mem. at 23 n.17. *Wilson* is not dispositive. In *Wilson*, the plaintiffs alleged that because of the defendants' positions as CEO and CFO of a company that made pickles, condiments, and frozen foods, the Court should have imputed knowledge to the defendants that the company's computer system may not have been able to track trade expenses and customer deductions, and that the defendants knew that any uncaptured customer deductions, once captured, would reveal a material difference in trade spending than had been originally estimated by the company. *Id.* at 641-42. The Court disagreed. *Id.* at 642.

By contrast, in the instant case, Plaintiffs are not claiming that Carr and Baldwin should have been aware of a nuanced accounting issue unrelated to the Company's core business (which, in *Wilson*, was canned-food sales).²³ Rather, at Heartland, data security is paramount to the Company's business,²⁴ and the Defendants held themselves out to be industry leaders in that field. *See, e.g.*, Compl. at ¶113. As such, given the importance of data security to the Company and to the market that it serves, Carr and Baldwin are presumed to know the truth about adverse facts existing during the Class Period relating to the security breach

²³ Interestingly, Defendants have never, either in the Motion or publicly, denied the well-pled allegation in the Complaint that they knew of the SQL Injection Attack prior to making the first Class Period statements in February 2008.

²⁴ Corroborating this fact is Defendants' own Motion at Exhibit A, wherein Defendants cite to fifteen separate disclosures made just in their March 10, 2008 10-K alone that relate to data security at Heartland. *See* Dkt. No. 20-4.

that occurred at the Company in 2007, and the pervasive security vulnerabilities on the Company's databases, as well as the exceedingly high likelihood they would negatively impact the Company's expected financial performance and stock price when the truth was revealed. *See In re Scottish Re Group Sec. Litig.*, 524 F. Supp. 2d 370, 394 (S.D.N.Y. 2007) ("It is simply not a plausible opposing inference that the Company's officers – sophisticated executives actively engaged in the planning of these transactions – were ignorant of the transactions' consequences on the Company's deferred tax assets.").

(3) Defendants Are Presumed to Know Facts About the Security Breach Based on Their Positions at Heartland

Tied closely to the so-called "core business" inference, the Complaint further establishes the scienter of Carr and Baldwin based on their high-ranking positions in the Company. The district court in *In re Countrywide Fin. Corp. Sec. Litig.*, 588 F. Supp. 2d 1132 (C.D. Cal. 2008) recently set forth the following principles governing a position-based inference of scienter:

(1) a defendant's position within the company is a relevant circumstance to consider in the *Tellabs* analysis; (2) all particularized allegations about a defendant's activities and statements should be considered before making a position-based inference, just as in any *Tellabs* analysis; and (3) position alone creates a strong inference of scienter only in the extraordinary case where it is 'absurd to suggest' that a defendant did not know.

Id. at 1191. In fact, as demonstrated above, this is precisely one of those cases where it is “absurd to suggest” that Carr or Baldwin, “by virtue of their positions, would not have knowledge of developments in core operations or important transactions.” *Id.*

Moreover, the Complaint demonstrates that Carr and Baldwin were the Company’s designated representatives for communicating with the market about Heartland’s operations, and more specifically, the safety and security of the Company’s databases. In numerous conference calls, they appeared to speak thoroughly and intelligently (albeit, falsely) with market analysts, responding in detail to questions about data security at Heartland. *See, e.g.*, Compl. at ¶¶93, 109. Given their role as Company spokesmen who made the misrepresentations here, it is “exceedingly unlikely” that Carr and Baldwin were unaware of the security problems at the Company, and were “merely repeating lies fed to him by other executives of the company.” *Tellabs II*, 513 F.3d at 711.

(4) Defendants’ Assertion that the February 13, 2008 Conference Call Does Not Evidence Fraudulent Intent Because Defendants were Discussing a Security Spend is a Red Herring

Defendants spend a page and a half of their brief arguing that the false and misleading statements cited by Plaintiffs in the Complaint from the February 13, 2008 conference call do not evidence fraudulent intent because Carr and Baldwin were discussing a fourth quarter 2007 security spend which was unrelated to any

purported security breach. *See* Def. Mem. at 16-17.²⁵ Defendants’ argument wholly ignores the wealth of case law that holds that when a corporation does make a disclosure – whether it is voluntary or required – there is a duty to be complete and accurate. *See Jaroslawicz v. Engelhard Corp.*, 704 F. Supp. 1296, 1299 (D.N.J. 1989); *Lautenberg Found. v. Madoff*, No. CIV.A. 09-816, 2009 WL 2928913, at *6 (D.N.J. Sept. 9, 2009). In other words, “[i]f ... a company chooses to reveal relevant, material information even though it had no duty to do so, it must disclose the whole truth.” *Grossman v. Waste Mgmt., Inc.*, 589 F. Supp. 395, 409 (N.D. Ill. 1984); *see also In re Allaire Corp. Sec. Litig.*, 224 F. Supp. 2d 319, 327 (D. Mass. 2002) (“[H]aving elected to comment on financial and product sales performance, [the company] was required to make full and accurate disclosures.”).

Regardless of whatever context Defendants want to try and provide for their February 13, 2008 statements, the allegations of the Complaint (which must be taken as true) allege that at the time of Defendants’ statements, Defendants were aware that a major security breach had occurred at the Company, and that the security breach had not been remedied. In that context, or any other context that Defendants want to provide, the statements made by Defendants on the February 13, 2008 conference call, including that “*it was nothing in terms of data security*

²⁵ Initially, the cause of the security spend at the Company in the fourth quarter 2007 is a fact issue that is not proper for resolution on a motion to dismiss.

external intrusion” in response to a question about whether an incident had occurred at the Company (*see* Compl. at ¶93), are false and misleading.

Once Defendants made disclosures concerning security vulnerabilities at the Company in the fourth quarter of 2007 and Defendants’ purported resolution of those matters, Defendants had a duty to make complete and full disclosure of the SQL Injection Attack on the Company’s systems during that quarter. *See, e.g., Flynn v. Bass Bros. Enters.*, 744 F.2d 978, 984 (3d Cir. 1984) (holding that a duty to speak arises when affirmative description of a tender offer is made); *Staffin v. Greenberg*, 672 F.2d 1196, 1202, 1204 (3d Cir. 1982) (holding that affirmative statements trigger a duty to speak). As such, Defendants’ assertion that the February 13, 2008 conference call does not evidence fraudulent intent because Defendants were discussing a security spend is without merit.

(5) Plaintiffs Do Not Plead that Carr’s Stock Transactions During the Class Period Evidence Fraudulent Intent

Defendants’ argument that their Class Period stock transactions negate any inference of scienter misses the mark. *See* Def. Mem. at 23-25. The Complaint does not allege that Carr’s stock sales during the Class Period evidence fraudulent intent. *See* Compl. at ¶¶117-119. Rather, the purpose of including Carr’s Class Period stock sales is to show that even after the Class Period, Defendants

attempted to continue to mislead the market as to their knowledge of the security breach.

Indeed, although Defendants had knowledge of the security breach in *December 2007*, the Company issued a statement after the Class Period indicating that at the time that Carr's 10b5-1 trading plan was announced (in *August 2008*), he was "*not in possession of any material non-public information concerning the Company*," and further that "*Heartland categorically denies that Mr. Carr was aware of a potential security breach at the time he adopted his trading plan.*" See Compl. at ¶118. As set forth above, and throughout the Complaint, these statements are false, and support an additional inference of scienter as to Defendants.

D. The Complaint Sufficiently Alleges Loss Causation

Pleading loss causation requires only a "short and plain statement" showing that "the pleader is entitled to relief." *Dura Pharms., Inc. v. Broudo*, 544 U.S. 336, 346 (2005) (quoting Fed. R. Civ. P. 8(a)). To satisfy Rule 8(a), plaintiffs need only allege "some indication of the loss and the causal connection" to defendants' alleged misstatements and omissions during the class period. *Id.* at 347. Whether the plaintiff has proven causation is usually reserved for the trier of fact. *Steiner v. MedQuist, Inc.*, No. 04-5487, 2006 U.S. Dist. LEXIS 71952, at *63 (D.N.J. Sept.

29, 2006); *EP Medsystems, Inc. v. EchoCath, Inc.*, 235 F.3d 865, 884 (3d Cir. 2000).

Moreover, a plaintiff can allege loss causation by pleading that the truth was revealed through a series of corrective, partial disclosures. *See In re Bradley Pharms., Inc. Sec. Litig.*, 421 F. Supp. 2d 822, 828-29 (D.N.J. 2006); *In re Enron Corp. Sec., Derivative & ERISA Litig.*, 439 F. Supp. 2d 692, 701 (S.D. Tex. 2006). To be corrective, a disclosure need only partially disclose the purported fraud. *See Dura*, 544 U.S. at 342. A plaintiff “is not necessarily precluded from establishing loss causation where a corrective disclosure does not, on its face, specifically identify or explicitly correct a previous representation, or expressly disclose the particular fraudulent scheme the plaintiff alleges.” *In re Motorola Sec. Litig.*, 505 F. Supp. 2d 501, 546 (D. Ill. 2007); *see also Bradley*, 421 F. Supp. 2d at 828. Moreover, “[a]s long as the misrepresentation is one substantial cause of the investment’s decline in value, other contributing forces will not bar recovery under the loss causation requirement” but will play a role “in determining recoverable damages.” *In re Daou Sys., Inc.*, 411 F.3d 1006, 1025 (9th Cir. 2005).

Here, Plaintiffs allege sufficient facts to show that Defendants’ misrepresentations proximately caused Plaintiffs’ losses. *See* Compl. at ¶¶129, 131. Heartland’s fraudulent statements presented a misleading picture of Heartland’s core business. *See* Compl. at ¶¶129-130. Through a series of partial

disclosure events regarding the December 2007 security breach, Heartland's stock prices dropped 8.16% on January 20, 2009 (when Heartland first disclosed that a security breach had occurred at the Company), 42% on January 22, 2009 (when the market became aware that the security breach may have involved more than 100 million accounts, doubling the largest card data theft in U.S. history), and 30.12% on February 24, 2009 (when Heartland disclosed the impact of the security breach on the Company's Fourth Quarter 2008 earnings and the uncertainties facing the Company concerning the costs relating to the security breach). *See* Compl. at ¶¶108-116, 133. Indeed, after trading at artificially inflated prices due to the misrepresentations and ongoing fraudulent conduct by Defendants, Heartland's stock had a total decline of almost 80% from its high during the Class Period. *Id.* This type of pleading to demonstrate loss causation was recently approved in *In re Par Pharm. Sec. Litig.*, C.A. No. 06-cv-3226 (PGS), 2009 U.S. Dist. LEXIS 90602, at *31 (D.N.J. Sept. 30, 2009). As such, Plaintiffs have adequately alleged loss causation.

Defendants' suggestion that Plaintiffs' allegations arguing that certain non-disclosures are not tied to Plaintiffs' losses are quite simply wrong. *See* Def. Mem. at 27-29. In *Dura*, the Supreme Court merely suggested that the plaintiffs need to have alleged in some fashion that the truth became known before the share price fell. *Dura* neither addressed what types of events or disclosures may reveal the

truth, nor explained how specific such disclosure must be. *Bradley*, 421 F. Supp. 2d at 828-29. The truth revealed in the January and February 2009 disclosures put the market on notice of Heartland's security breach, its effect upon the Company, and upon the misrepresentations connected to the same. Plaintiffs have sufficiently alleged loss causation with respect to the Class Period misrepresentations tied to the security breach at Heartland. *See, e.g., Par Pharm.*, 2009 U.S. Dist. LEXIS 90602, at *31; *In re Tommy Hilfiger Sec. Litig.*, No. 04-Civ-7678, 2007 U.S. Dist. LEXIS 55088, at *7-*9 (S.D.N.Y. July 20, 2007).

E. The Complaint Sufficiently Alleges Control Person Liability

Carr and Baldwin contend Plaintiffs' §20(a) claim should be dismissed because Plaintiff fails to plead an underlying violation of Section 10(b) or Rule 10b-5. *See* Def. Mem. at 30. This assertion is meritless. Without rehashing the arguments discussed above, Plaintiffs have alleged primary violations under 10(b), including sufficient allegations that Carr and Baldwin acted with the requisite scienter. Accordingly, the Court should sustain Plaintiffs' control person liability claims under §20(a). *See, e.g., Sheehan v. Little Switzerland, Inc.*, 136 F. Supp. 2d 301, 315 (D. Del. 2001); *Wiley v. Hughes Capital Corp.*, 746 F. Supp. 1264, 1283 (D.N.J. 1990).

III. CONCLUSION

As discussed herein, Plaintiffs have pled their claims pursuant to §§10(b) and 20(a) of the Exchange Act consistent with Rule 8, Rule 9(b) and the PSLRA. Accordingly, Defendants' Motion should be denied in its entirety.

DATED: October 26, 2009

COHN LIFLAND PEARLMAN
HERRMANN & KNOPF LLP
PETER S. PEARLMAN

s/Peter S. Pearlman

PETER S. PEARLMAN

Park 80 Plaza West-One
Saddle Brook, NJ 07663
Telephone: 201/845-9600
201/845-9423 (fax)

Liaison Counsel

COUGHLIN STOIA GELLER
RUDMAN & ROBBINS LLP
PAUL J. GELLER
DAVID J. GEORGE
JAMES L. DAVIDSON
BAILIE L. HEIKKINEN
120 E. Palmetto Park Road, Suite 500
Boca Raton, FL 33432-4809
Telephone: 561/750-3000
561/750-3364 (fax)

FARUQI & FARUQI, LLP
NADEEM FARUQI
EMILY C. KOMLOSSY
JAMIE R. MOGIL
369 Lexington Avenue, 10th Floor
New York, NY 10017-6531
Telephone: 212/983-9330
212/983-9331 (fax)

Co-Lead Counsel for Plaintiffs